

Electronic Money: A viable payment system?

Andres Guadamuz¹

¹ School of Law

University of Edinburgh
Old College, South Bridge
Edinburgh EH8 9YL
United Kingdom

Keywords: e-commerce, payment systems, online payments, cash, e-cash, financial services, Mondex, electronic money, software money, EU Directive, money institutions.

Abstract. This paper explores some of the legal and practical issues related to the implementation of electronic money placed in smart cards as a viable online payment system. This is a subject of particular importance as many there are many hopes from the financial industry about the implementation of an electronic currency system will create a great method for small transactions, both online and offline.

Introduction

There has been a lot of interest in recent years in the development of electronic money, which promises to be one of the greatest revolutions in payment systems since the development of money itself. This development has been in the making for quite some time now, from the inception of bank cheques to the creation of credit cards and the implementation of electronic money transfers, financial services practices and new technology has been coming together to produce the greatest leap in the way in which we conduct our everyday monetary transactions. The implications of the wider acceptance of an electronic money scheme would have incredible effects in our lives, and very possibly, in the future development of electronic commerce as a means of distance selling. Electronic money could possibly serve to diminish the constant apprehension of consumers to transacting online for fears that third parties will misuse their credit card details.

The recent passing of a European Directive that regulates electronic money institutions has served to establish the legal recognition of such monumental change, and has also served to legitimise the efforts of creating such payment systems. Economists, regulators, government institutions and businesses appear to be gearing themselves as well for the possible explosion of electronic money into everyday life. However, despite such warm recognition and favourable reception by so many sectors of the economy, there are still very palpable concerns about the eventual implementation of this scheme. Trials seem to come and go, and no dates are given on when we can expect to see any further developments in this area. Why is this?

There cannot be any doubt that such momentous task must be met with caution, mostly because the security issues have not been widely put to rest. This paper will attempt to explore some of these issues, and will try to analyse if these security concerns are enough to make electronic money a failed experiment, yet another rarity in the ever-changing world of finances.

Electronic money

Definition. Electronic money is nothing more than the replacement of physical cash in the shape of coins and banknotes with an electronic equivalent. According to Wikipedia, digital cash is:

“A system that allows a person to pay for goods or services by transmitting a number from one computer to another. Like the serial numbers on real dollar bills, the digital cash numbers are unique. Each one is issued by a bank and represents a specified sum of real money. One of the key features of digital cash is that, like real cash, it is anonymous and reusable.” [1]

From this definition it is obvious that electronic money is very much like physical money for all practical purposes. It is anonymous; it is given value by a financial institution; and it must be subject to be used to pay for goods and services in any sort of transaction. The new Electronic Money Institutions European Directive—which will be discussed in more detail later—also defines electronic money for the purpose of the legal regime that will regulate this emerging sector. It states that:

“‘electronic money’ shall mean monetary value as represented by a claim on the issuer which is:
(i) stored on an electronic device;
(ii) issued on receipt of funds of an amount not less in value than the monetary value issued;
(iii) accepted as means of payment by undertakings other than the issuer.” [2]

This definition is wide ranging, and attempts to be technology neutral. The requirements for a payment system to be considered electronic money are all there.

a) The electronic cash must have monetary value, which assumes that schemes such as store reward points will not apply to this definition. This would also exclude so-called “Internet cash” payment systems, such as Beenz, Flooz or Digicash. These systems created a proprietary currency useable only in participating merchants. The complexity of these systems and the fact that these points could only be used in several places doomed this scheme, and most of these systems no longer exist. [3]

b) The fact that it presents a “*claim on the issuer*” means that the issuer of the money must accept it and provide the equivalent of the monetary value back to the bearer.

c) The main difference with physical money is that it must be stored in an electronic medium, but the definition does not specify what type. It must be assumed that this means cards, PDAs, mobile phones, personal computers and any other electronic device.

d) The value stored in an electronic money device must not be any less than the monetary value issued, which means that there must not be any charges for usage, such as interest rates or usage charges in traditional credit cards. This also assumes that the value of the purchase should not be superior to the amount specified in the money, if it was then it should be considered a credit device, and thus subject of an entirely different regulatory system. [4]

e) The payment system must be accepted by merchants other than the issuer, which means that it must have wider acceptance. This also makes a difference to store reward cards, which can usually be redeemed only by the issuing merchant.

Existing methods. Because the definition of electronic money is so broad as to include any sort of electronic device to store monetary value, the methods of electronic money are only limited to the existing technology. At present there are two main storage methods for electronic money, by software and by cards.

The method of software money is a payment system where money is stored in a computer hard drive by means of a proprietary software program. [5] The program creates an electronic wallet that is charged with money from a bank account, and then the user can purchase goods or services by sending the information via this electronic method. The transaction is encrypted and the identity of the user is kept hidden from the merchant. [6] There are several companies offering software like this, but it has not proven to be extremely popular. One of the main companies pushing this scheme was DigiCash, with which the customer could download a small program to store money in their computers. DigiCash proved to be a disappointment and has been purchased by another company called Ecash. Other software money schemes exist, but suffer from the same lack of interest by consumers. [7]

The most viable and promising electronic money system is that of storing monetary value in secure cards with microchips, known as smart cards. The smart card is simply put, *“a plastic rectangle containing an electronic chip, and holding a certain amount of readable data.”* [8] This technology is not only circumscribed to electronic payment systems, it is also to be found in several other areas such as digital television boxes and Subscriber Identity Module (SIM) cards for mobile phones. Smart cards for electronic payments use the chip to store certain amount of value, which can be charged in anything from a public phone to an Automated Teller Machine (ATM). [9] For security reasons, the information in the card must be stored by use of encryption algorithms that can only be decoded by an adequate reader; otherwise the value from the card cannot be unlocked. The bearer will present the card to a retailer that has a card reader, and the value will be then unlocked and transferred to their account. This value is redeemable with the card issuer. Smart cards can also be used for Internet transactions if the consumer has a card reader attached to their computer, this reader will unlock the value in the card and send the information to the online retailer, facilitating an anonymous e-commerce transaction.

There are several smart cards schemes under development, such as Proton, Mondex and VisaCash; each trying to take the initiative in this competitive new market. At the moment the scheme that seems more likely to advance is Mondex, which started as an initiative of the National Westminster Bank (NatWest) in the United Kingdom, and has later received the support of the credit card company Master Card. This scheme has a large number of affiliates in several countries around the world, and the companies involved hope to make Mondex into the next electronic money standard around the world. [10]

Advantages and disadvantages of electronic money

It is important to consider the advantages and disadvantages of electronic money because these schemes are set to become the future replacement of physical cash. A brief description of these will be seen now.

Advantages. Perhaps one of the main advantages of the proposed system is for the issuing banks. The credit card and debit card payment systems that are in effect are costly, as they require a complex system of contractual and operational interactions between consumers, retailers and issuers. Another factor that elevates the cost of this

system —and in particular in credit card payments— is that consumers have to be credit worthy in order to receive credit. This means that the cost of those who do not pay back credit is transferred to other consumers in the shape of interest rates. One of the results of this high cost is that this payment system is not efficient for micro-payment systems, such as those that are increasingly popular on the Internet with the adoption of pay-per-use schemes such as digital music, e-books and Internet performances. [11]

In contrast to this, electronic money works in a much simpler and cheaper way, which makes it ideal for micro-payments and thus much more attractive for credit companies. The low cost of electronic money is that it does not require the huge amount of expensive infrastructure that other systems do, in particular credit cards, because the value in a card can be transferred into a reader without need to contact a network facility to corroborate the payment, the transaction can be performed locally and the money will stay in the reader until later download. [12]

Several authors have pointed out many of the advantages of the electronic money model. Some of these are:

- *Consumer convenience*: Electronic money could prove very convenient for consumers. Because it involves advanced charge of money from the owner's bank account, almost anybody can be supplied with a smart card, as there is no risk to the issuer. Consumers will also find it useful to have to do without carrying cash for small transactions, such as bus fares. [13]
- *Increased consumer confidence*: Because a smart card only holds the amount of money that the bearer has placed on it, consumers will be more willing to use it to purchase over the Internet without fear of somebody else misusing the payment information, as happens with credit card fraud. Some of the schemes are also being issued with a built in locking code, which will allow users to lock the cash on a card, making sure that if the card gets lost or stolen another person will not be able to use the money. [14]
- *Payer anonymity*: The payer can remain anonymous, as is the case with paying in cash.
- *Issuer advantages*: As it has been mentioned, this system is much cheaper to operate than other payment models, which is a great advantage for issuing institutions. The liability for the issuer is also minimal, which reduces costs and enhances profits. [15]

Disadvantages. Although the potential advantages for electronic money are considerable, there are still several problems that should provide a healthy dose of skepticism for this payment system.

- *Consumer confusion*: With three schemes competing to become the electronic money standard, there is a real possibility of the whole system becoming too complicated for users. One of the main problems with too many schemes would be that the user may not be able to use the card everywhere, which is what would be expected of a system that is meant to replace physical currency.
- *Regulatory maze*: As it will be seen later, the regulation for electronic money is still unclear in some vital points, which must be answered before the system is made more widely available.
- *Security*: The main concern that must exist in the minds of those interested in the implementation of electronic cash must be security. As happens with physical cash, widespread counterfeiting of electronic currency could have huge

implications for the economy. Security will receive a more detailed treatment in a later section.

Regulatory framework

It should not come as a surprise that the electronic money payment system already has generated legislative interest, despite of its relative youth. At least in the European Union this interest has even gone as far as to the passing of a European directive on the subject, but for the moment it has been ignored by some others.

European regulation. The main regulatory tool in the European Union is the Directive 2000/46/EC on electronic money institutions, also known as the EMI Directive. This piece of legislation is perhaps one of the most important developments for the field of electronic payments in recent years, as it sets the stage for the eventual rollout of electronic money schemes across the European Union.

The directive starts by usefully defining what electronic money is, a definition that has already been covered in an earlier section. [16] A very important point made by the directive is that it does not apply directly to deposit-taking or credit-giving institutions (banks) as defined by the First Banking Directive, [17] which will be regulated by banking regulations. The directive then will only apply to non-banking institutions that issue electronic money, and states clearly that member countries will forbid any other person or undertaking that does not fall into those categories from issuing electronic money. [18] This is rather confusing and circular, as it would seem that the directive has defined as electronic money institutions those that issue electronic money. At the same time, the directive will amend the existing Banking regulations to include electronic money institutions into their scope. According to Chuah, the reason for this provision is that it will allow electronic money institutions to benefit from the single passport license rule that exists in European banking regulation, which allows banks to operate all around the European Union if they are licensed in one of the member states. [19]

The EMI Directive goes on to establish the actions which an electronic money institution will be able to perform other than issuing money, which amount mostly to administration or operational functions. This is important because it specifies that non-banking financial institutions will not be excluded from this, but it makes sure that they will not take deposit or give credit, which would turn them into banks and thus subject to the complex banking regulatory system. [20]

There are many other important provisions:

- The electronic money must be redeemable from the issuer at any time in bank notes or coins, and the contracts should always be clear about the conditions of redemption (Art 3).
- Electronic money institutions must have an initial capital of one million euros, and their own funds shall not fall below that amount. At any time, the institution must own funds that are equal or above 2% of the average total amount of their financial liabilities for the previous six months (Art. 4).
- These institutions should have investments of an amount of no less than their financial liabilities in electronic money, and the operation of the institution should be sound and prudent. (Arts. 5-6)
- Electronic money institutions will be subjected to money laundering regulations.

As complete as the EMI Directive is, there are still several issues that are left in a regulatory limbo, in particular those about liability for loss and misuse of the card. The original recommendations from the European Commission contained several rules about responsibilities and liabilities that have not made it to the actual directive. [21] Among these recommendations the holder would be liable for the loss of the card, and would be liable for an amount of up to 150 EUR for the misuse of the card. The issuer would be liable for any security breach or failure in the card that would result in loss of value attributable to the issuer. It would seem that these provisions will be left to the individual countries to sort out by legislation or even by self-regulation. Newman and Sutter point out that the latter is the case with UK, as there are some liability provisions included in the Banking Code, the self-regulation code of practice for British financial services. They point out that the liabilities of the holder of any electronic purse will not exceed £50 GBP. [22] Some of these problems will need to be sorted out if electronic money is to become widespread.

United Kingdom. The United Kingdom has recently adopted the EMI Directive with the Electronic Money Regulations 2002. [23] The regulatory regime in the UK will be the responsibility of the Financial Services Authority (FSA), which will have the power to decide when an institution is to be considered as an issuer of electronic money. The Financial Services and Markets Act 2000 has been amended by the new regulations to accommodate electronic money institutions under its regulatory framework.

The HM Treasury has also issued the results of a consultation paper that criticised the definition of electronic money in the EMI Directive as being too narrow. [24] Because of this, the Treasury recommends that the FSA should have the power to decide on an *ad hoc* basis whether a payment scheme should be considered as an electronic money institution and be subject to the regulation contained in it.

Other Countries. There has not been a lot of regulatory activity in regards to electronic money outside of the European Union, which should not be surprising given its relative youth. However, there has been no shortage of proposals and calls for regulation from several sectors in various countries, stemming from the fact that this field represents a potential legal minefield for countries that have not thought out this phenomenon thoroughly.

Australia has in place some legislation that could be used as an initial regulatory framework for electronic money. This is the Payment Systems (Regulation) Act 1998, [25] which directs the Reserve Bank of Australia to authorise and oversee payment schemes, known as purchased payment facilities (PPF). The definition of a PPF according to this Act states that it will be any payment system other than cash where:

“*a) the facility is purchased by a person from another person; and*
(b) the facility is able to be used as a means of making payments up to the amount that, from time to time, is available for use under the conditions applying to the facility; and
(c) those payments are to be made by the provider of the facility or by a person acting under an arrangement with the provider (rather than by the user of the facility).”[26]

Although this is not geared specifically to electronic money, it could be argued that this new type of payment falls under the definition presented by this article while a specific piece of legislation is passed. [27]

The United States has not yet started to consider a legislative solution for electronic money, and some legal experts are complaining that at the moment the road is filled with regulatory inconsistencies. Examples of these abound. The Federal Deposit Insurance Corporation has ruled that deposits transferred into a value card lose their insurance status, an opinion that would have immense implications for the eventual success of electronic money stored in a smart card. The Department of Justice has been looking at some e-money schemes; in particular their Antitrust Division is concerned about the possible monopolistic implications of such payment models. [28] Some of these worrying discrepancies could be ironed out by umbrella legislation similar to the European directive, which is something that may be considered by legislators and regulators in the United States.

Is electronic money secure?

As it was expressed earlier, the main obstacle towards the widespread implementation of electronic money as a replacement to cash is that of the existence of serious security concerns. Security worries cannot be underestimated when talking about this very important area, after all, a security breach which allows people to hack into a smart card and place whatever value they see fit to it would have huge repercussions for the economy, which would be the same as widespread counterfeiting of money. In fact, counterfeiting has been shown to be such an economic worry that it receives some of the highest law enforcement in the world, as it has the potential of creating runaway inflation and to generally reduce the value of money in a country. [29]

It must be said that the potential for misuse of smart cards is considerable, and it could account for the relative slowness with which the rollout of electronic model schemes has been developing. With several trials underway around the world, security concerns have only increased.

As soon as the electronic money seemed like a possibility on the horizon, several security experts warned that storing value on smart cards was vulnerable to hacking attacks. [30] This threat was dismissed originally as scaremongering, but it was only a short while before the embedded encryption a security-consulting firm broke security of the Mondex card. The story was first made public by a leaked note from the National Bank of New Zealand about the card being used in one of the Mondex trials in England. In this note, officials at the bank expressed concerns about a report by the Dutch security Consultancy firm TNO that specified that the encryption had been broken. The report was immediately made public on the Internet and was later corroborated by the bank. [31] Soon after this, rumours were flying around the web about just how vulnerable the early chips used were, including several stories about the possibility of using a microwave oven and a calculator to charge the cards with several hundreds of pounds. [32]

A very telling indication about the level of fear that the potential vulnerability of electronic money has is that most of the trials have been running in very small communities where a cancellation of the program would be easier if security has been compromised. [33]

Security concerns remain, as chip hackers assure that they can probably hack any sort of technology thrown at them. As the cards will also be protected by strong encryption, it would be possible that large criminal organisations could employ cryptographers to try to break the security systems.

But not actual security is of concern; the consumer perception of security should also be taken into consideration. If consumers are scared of using the system because of security reasons, the system could easily fail. [34]

Conclusion

There is no doubt that smart cards have an immense potential to become the largest method for payment in the world, eventually replacing physical currency. The law would appear to be taking this seriously enough in some countries, and it is encouraging that there are already enough regulatory efforts to attempt to make legal sense of this payment method. The potential advantages for consumers, merchants and financial services make electronic money the way to go in the future. Nevertheless, there cannot be any sort of complacency when trying to make this system as secure as humanly possible, the consequences otherwise would be terrible to consider.

The electronic money industry must make sure that this payment system does not make it out of the door without the utmost certainty that the system is as secure as it can possibly be. So far the number of trials in towns and small cities around the world would show that they are indeed taking these threats seriously.

References

- [1] Webopedia. *Digital Cash*. @: <http://www.webopedia.com/TERM/D/digital_cash.html>
- [2] Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions. O.J.E.C. L275/39, 27/10/2002.
- [3] For more on the Internet money collapse, see: J. Kornblum. "Internet currency: You Flooz, you may lose". *USA Today*, (August 22, 2001). @: <<http://www.usatoday.com/life/cyber/tech/2001-08-22-ebrief.htm>>
- [4] For some of the regulatory regimes for credit cards, see: E. P. Ellinger, E. Lomnicka and R. Hooley. *Modern Banking Law*, (Oxford University Press, England 2002), pp. 532-536.
- [5] J. Chuah. "The New EU Directives to regulate electronic money institutions - A critique". *Journal of International Banking Law*, (2000), 15(8), pp. 181-182.
- [6] P. Robertson. "Internet Payments". *Law of Bank Payments*, M. Brindle and R. Cox editors, (Sweet & Maxwell, London 1999), pp. 251-253.
- [7] Some software money schemes are Ecash: <<http://www.ecash.com/online/>>; CyberCash: <<http://www.cybercash.com>> and NetCash <<http://www.netbank.com/~netcash>>
- [8] S. Newman. "Introduction: Smart Cards". *Smart Cards*, S. Newman editor (ECLIP II, IST Project Report 1999), p. 3.
- [9] L. Edgar. "Electronic Money". *Cross Border Electronic Banking: Challenges and Opportunities*. C. Reed, I. Walden and L. Edgar editors, 2nd edition (LLP, London 2000), p. 203.
- [10] For more on the Mondex scheme, see: J. Finlayson-Brown. "Mondex: Structure of a new payment scheme". *Journal of International Banking Law* (1997), 12(9), pp. 362-366).
- [11] S. Miller. "Payment in an online world". *Law & the Internet: a framework for electronic commerce law*. L. Edwards and C. Waelde, editors, (Hart Publishing, London 2000), pp. 74-75.
- [12] Finlayson-Brown, op. cit; pp. 363-364.
- [13] Miller, op. cit; p. 75.
- [14] Ibid.
- [15] T. Tether. "Payment systems for E-commerce". *Border Electronic Banking: Challenges and Opportunities*. C. Reed, I. Walden and L. Edgar editors, op. cit; pp. 194-195.
- [16] Supra, note 2.

- [17] Directive 2000/12/EC of the European Parliament and of the Council of 20 March 2000 relating to the taking up and pursuit of business of credit institutions; O.J.E.C. L126/1, 26/5/2000.
- [18] Art. 1.4.
- [19] Chuah, op. cit; p. 182.
- [20] Ibid; p. 183.
- [21] Commission Recommendation (97/489/EC) of 30 July 1997 concerning transactions by electronic payment instruments and in particular the relationship between issuer and holder; O.J.E.C. L208/52, 02/08/1997.
- [22] S. Newman and G. Sutter. *Electronic Payments: The Smart Card, Computer Law & Security Report* (Vol. 18, Issue 5, 1/10/2002), pp. 307-313.
- [23] *The Electronic Money (Miscellaneous Amendments) Regulations 2002*, No. 765.
- [24] HM Treasury. Implementation of the Electronic Money Directive: A consultation document, (October 2001), @: <http://www.hm-treasury.gov.uk/mediastore/otherfiles/e_money.pdf>
- [25] *Payment Systems (Regulation) Act*. No. 58, 1998.
- [26] Ibid; s. 9(1).
- [27] For more on the Australian legislation, see: J. Forder and P. Quirk. *Electronic Commerce and the Law*, (John Wiley & sons, Australia 2001) p. 129.
- [28] E. Harris Solomon. "What should regulators do about consolidation and electronic money?" *Journal of Banking & Finance* 23 (1999), p. 650.
- [29] For more about counterfeiting, see: E. Groseclose. *America's Money Machine: Story of the Federal Reserve*, (Crown Publishing, New York 1980).
- [30] D. Bank. "Smart Cards Are Open to New Attack by Hackers, Say Israeli Researchers", *Wall Street Journal* (October 21, 1996), p. A17.
- [31] R. Brown. "Leaked National Bank memo confirms pilot version of Mondex broken", *Computerworld News Wire* (September 15, 1997), @: <<http://insight.mcmaster.ca/org/efc/pages/media/nz-computerworld.15sep97.html>>
- [32] For one of these reports, see: <<http://www.s-t.com/daily/10-96/10-20-96/f05bu035.htm>>
- [33] For more details about the trials, see: B. A. Good. *Electronic Money*, Federal Bank Reserve of Cleveland Working Paper, 96/17, @: <<http://www.clev.frb.org/research/workpaper/1997/wp9716.pdf>>
- [34] Some of these concerns were experienced in a failed trial of a cashcard program performed by four Swedish banks in the north of that country. For more on this, see: J. Holmström and F. Stadler. "Drifting technologies and multi-purpose networks: the case of the Swedish cashcard", *Information and Organisation* 11 (2001), pp. 187-206.